Adobe® Connect™ technical overview

Adobe Connect is a rich web conferencing system that enables secure online meetings, training, and webinars that anyone can access through any web browser. It allows nontechnical subject matter experts to easily create online meetings and web communications that include voice, video, animations, and interactive multimedia that participants view using the Adobe Flash® Player runtime in a browser or from native mobile applications.

Modular architecture
Adobe Connect Server is the foundation of Adobe Connect. It uses a highly scalable, secure, and flexible architecture that enables people to collaborate in real time no matter where they are. It also allows people to access marketing, sales, and training materials at their own convenience through on-demand presentations. Adobe Connect Server offers enterprise-class scalability, with support for single-server and clustered environments. It provides reliable redundant deployment that can support thousands of concurrent users. Designed as an open platform, it can be extended and integrated with other systems through a comprehensive set of APIs. This guide presents a technical overview of Adobe Connect Server architecture for various deployment scenarios.

Table of contents
1 Modular architecture
2 Adobe Connect Server components
4 Client connection—data flow
5 Hosted, licensed, and managed services solutions
8 Enterprise integration
12 Extensibility and custom integration
14 Adobe Connect Edge Server
16 Deploying servers in a cluster
18 Security
20 Adobe Connect bandwidth requirements

Adobe Connect

<table>
<thead>
<tr>
<th>Adobe Connect Meeting</th>
<th>Adobe Connect Training</th>
<th>Adobe Connect Events</th>
<th>Adobe Presenter</th>
</tr>
</thead>
</table>

Adobe Connect Server or Hosted

Access control
- Authentication
- Role-based permissions
- Group management
- Multi-tiered access
- Permissions

Reporting
- Permission-based access
- Dashboard reports
- Customizable reports
- Manager and group reports
- Cost center reports

User management
- User profile management
- Group management
- Session management
- Directory service integration

Scalability
- Clustering
- Failover
- Load-balancer support
- Backup storage support
- Edge servers

Delivery
- Rapid publishing
- Real-time data, voice
- Audio streaming
- Progressive downloads
- HTTP tunneling

Integration
- Web services
- Provisioning
- Application management
- Single sign-on
- Database-level reporting views

Security
- Flash technology
- TSL/SSL security
- Hashed passwords
- Privacy certifications

Compliance
- Administrator control
- Disable functionality
- Data recording and retention
- Rule-based access controls

Extensibility
- Flash
- Collaboration Builder SDK
- LDAP
- Web services
Adobe Connect Server components

Application suite
Adobe Connect Server offers a suite of applications that can be combined to meet your needs. It also includes a web-based interface that lets you manage users, permissions, and most account settings.

Adobe Connect Server includes three applications with features for meetings, training, and events. You can publish training content and multimedia presentations directly to the server from other products like Adobe Presenter and Adobe Captivate. You can also extend Adobe Connect Server and integrate it with other systems through its web services API and available software development kit (SDK). Adobe Connect Meeting—Conduct online meetings and seminars. Presenters can show multimedia presentations, share their screen, and broadcast live audio and video to participants in real time.

Adobe Connect Training—Create, manage, deploy, and track eLearning courses and curriculums, complete with enrollment, assessments, surveys, learner management, and reporting.

Adobe Connect Events—Manage the full life cycle of large- and small-scale events, such as email notification, event catalogs, registration management, reporting, and analytics.

Adobe Presenter—Rapidly create eLearning content and high-quality, multimedia, on-demand presentations that can include narration, quizzes, and video.

Adobe Connect Central—Manage account-related information and content with this web-based application. Use Adobe Connect Central to create meetings, manage presentations, create curriculums and events, view and download reports, and more.

Server architecture
Adobe Connect Server is a multi-tier server, separating logical functions such as presentation, application processing, and data management across independent processes.

<table>
<thead>
<tr>
<th>Functional Tier</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server</td>
<td>Apache</td>
</tr>
<tr>
<td>Application Server</td>
<td>Apache Tomcat</td>
</tr>
<tr>
<td>Streaming Server</td>
<td>Adobe Media Server</td>
</tr>
<tr>
<td>Database</td>
<td>Microsoft SQL Server</td>
</tr>
<tr>
<td>HTML Authoring/Publishing</td>
<td>Adobe CQ Server</td>
</tr>
<tr>
<td>Analytics</td>
<td>Adobe SiteCatalyst</td>
</tr>
<tr>
<td>Media Transcoding</td>
<td>Oracle Java^</td>
</tr>
</tbody>
</table>

Application server
Adobe Connect Server is built on J2EE using Apache Tomcat for the application layer. Apache HTTP Server provides the web server functionality. The server contains and executes all the business logic necessary for delivering content to users.

The Adobe Connect application server manages users, groups, on-demand content, and client sessions, among other tasks.

Some of the application server’s specific duties include access control, security, compliance, quotas, licensing, and auditing and management functions such as clustering, failover, and replication. It also transcodes media, such as Microsoft PowerPoint and Adobe PDF, to Flash format to allow viewing without the original application.

The Adobe Connect application server is stateless and follows a service-oriented architecture (SOA). Because the application server is stateless, scaling is near linear. The transactional and application metadata that the application server manages can be stored in either single or multiple replicated SQL databases.
Streaming communication server
Adobe Connect Server includes an embedded instance of Adobe Media Server that acts as the meeting server. This component handles all the real-time streaming of audio and video, synchronization of data, and delivery of rich media content. Adobe Media Server also plays a vital role in reducing server load and latency by caching frequently accessed streams and shared data.

Adobe Media Server uses the Real-Time Messaging Protocol (RTMP) but can be configured to use Secure Sockets Layer (SSL) for increased data security.

Database
The Adobe Connect Server database is used for persistent storage of transactional and application metadata, including user, group, content, and reporting information. Adobe Connect Server can use either the embedded database engine (Microsoft SQL Server Express) or the full version of Microsoft SQL Server. Check the Adobe Connect system requirements for the most up-to-date information. The embedded database engine must be installed on the same computer as Adobe Connect Server.

When Adobe Connect Server is deployed in a cluster, or with multiprocessor computers with Hyper-Threading Technology (HTT), you must use the full version of Microsoft SQL Server, and it cannot be installed on the same computer as Adobe Connect Server. Standard cluster and hot-swap configurations for Microsoft SQL database are supported for scalability and failover.

HTML authoring and publishing
Adobe Connect Server uses Adobe CQ, a web content management system, for creating and managing HTML-based templates used for event email notifications, landing pages, and user self-registration. It provides the ability to author and subsequently publish web pages. Adobe CQ requires at least one author and one publish instance within the Adobe Connect Server deployment when the Adobe Connect Events module is enabled. All the web page authoring related work is done in the Adobe CQ author instance and replicated in the publish instance. The publish instance is the read-only view of the web pages that have been authored in the Adobe CQ author instance. Multiple Adobe CQ author and publish instances can be configured within a server cluster to provide increased scalability and failover.

Analytics
Adobe Connect Server can provide extensive participant behavior reports and session analysis using the hosted Adobe SiteCatalyst service. These reports track viewing of landing pages; response to registration questions; attendance at meetings, webinars, or training; and even participation in polls, Q&A, and file download activity during meetings. The reports are only available for activities that have been published using the Adobe Connect Events module. Basic reports are included through a limited SiteCatalyst integration for both hosted and managed services deployments of Adobe Connect accounts. Advanced reporting requires a separately purchased SiteCatalyst account but can be enabled on any type of Adobe Connect Server deployment.

See Appendix B for SiteCatalyst variable mapping.

Media transcoding
Adobe Connect Server provides a number of file conversion utilities to automatically convert popular document formats into highest-quality files that are displayed in the meeting room. Files from PowerPoint (PPT, PPTX) are converted into small, vector-based files. This conversion provides the highest-quality, resolution-independent display for all participants. The conversion also faithfully reproduces hyperlinks and virtually all the original animations contained within each slide. When loaded into a meeting room, the individual slides are precached by each client to ensure the lowest latency transitions, requiring minimal bandwidth to maintain synchronization across all users. Animations are displayed as they were in the original slides and hyperlinks can be clicked. Other supported file formats such as PDF are similarly converted.
Client connection—data flow
Adobe Connect Server uses the following communication protocols: HTTP, HTTPS, RTMP, and RTMPS. RTMP is optimized to deliver real-time, rich media streams. RTMPS is the secure implementation of RTMP.

Unencrypted connections are made over HTTP and RTMP and follow the paths described in the following table. The numbers in the table correspond to the numbers in the data flow diagram.

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The client web browser requests a meeting or content URL over HTTP:80.</td>
</tr>
<tr>
<td>2</td>
<td>The web server responds and transfers the content or provides the client with information to connect to the meeting.</td>
</tr>
<tr>
<td>3</td>
<td>The client Flash Player requests a connection to the meeting over RTMP:1935.</td>
</tr>
<tr>
<td>4</td>
<td>Adobe Media Server responds and opens a persistent connection for Adobe Connect streaming traffic.</td>
</tr>
<tr>
<td>3a</td>
<td>The client Flash Player requests a connection to the meeting but can only connect over RTMPT:443.</td>
</tr>
<tr>
<td>4a</td>
<td>Adobe Media Server responds and opens a tunneled connection for Adobe Connect streaming traffic.</td>
</tr>
</tbody>
</table>

Encrypted connections are made over HTTPS and RTMPS and follow the paths described in the following table. The letters in the table correspond to the letters in the data flow diagram.

<table>
<thead>
<tr>
<th>Letter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>The client web browser requests a meeting or content URL over a secure connection on HTTPS:443.</td>
</tr>
<tr>
<td>B</td>
<td>The web server responds and transfers the content over a secure connection or provides the client with information to connect to the meeting securely.</td>
</tr>
<tr>
<td>C</td>
<td>The client Flash Player requests a secure connection to Adobe Media Server over RTMPS:443.</td>
</tr>
<tr>
<td>D</td>
<td>Adobe Media Server responds and opens a secure, persistent connection for Adobe Connect streaming traffic.</td>
</tr>
</tbody>
</table>
A client initiates the first connection to the application server. These connections, such as for login requests, file publishing, or content and event management, are made through HTTP or HTTPS. After the client engages in real-time communication, a connection to Adobe Media Server is started, and the Adobe Connect Server uses either RTMP or RTMPS to deliver streamed content.

By default, RTMP travels over port 1935 and is used for live interactions in an Adobe Connect meeting (video, voice, and screen sharing). HTTP traffic travels over port 80 and is used for client login and to transfer content (slides, documents, and so on). A connection uses RTMPT over port 443 if a connection through port 1935 is not successful or RTMPS on 443 if the server is configured to use SSL encryption. RTMPT uses HTTP tunneling, which negatively affects streaming performance.

For licensed deployments, you can customize the enterprise server communication ports to resolve cases in which corporate proxy servers and firewalls block port 1935 for inbound and outbound traffic on the LAN.

Mobile client connection—data flow
The Adobe Connect Mobile client is a native application available on platforms such as Apple iOS, Google Android, and others. This application allows devices on those platforms to log in, participate in, and even host meetings directly from the mobile device.

Adobe Connect Mobile can communicate over Wi-Fi or mobile networks and so is optimized to use less bandwidth than a full PC client for select activities.

The mobile client uses the same HTTP/HTTPS protocols and ports for login and authentication and the same streaming protocols and ports for real-time meeting data, as the standard meeting client.

Hosted, licensed, and managed services solutions
An Adobe Connect account can be accessed using any of three deployment models. For the greatest ease of deployment, an account can be hosted by Adobe in one of our many secure, multi-tenant clusters deployed around the world. You can also purchase the server software and deploy on your own hardware behind your firewall for ultimate security, control, and integration. Or to enjoy ease of deployment without sacrificing any integration options, Adobe and key partners offer a single-tenant managed service, hosting a server in a dedicated location with the option to allow VPN access to your internal data systems and custom configuration settings.

Hosted solution
The Adobe Connect hosted solution is an easy way for organizations to use the Adobe feature-rich web conferencing system without having to install or manage the software. Clients can manage, view, and participate in on-demand or live web presentations and training from anywhere in the world. The Adobe Connect hosted model provides the following advantages:

- Immediate account access, without having to set up and configure servers on-site
- Lower initial investment
- Service updates, infrastructure upgrades, and routine maintenance
- Reliable, redundant deployment with automated failover provisions
- Scalable deployment from a high-bandwidth Tier 1 hosting center

The Adobe Connect hosted database stores account metadata such as users, groups, event and meeting details, and content access. Microsoft SQL Server is used as the enterprise database solution for Adobe Connect hosted and is implemented with redundant database nodes to ensure high availability.

Adobe Connect hosted maintains documented and tested system recovery plans in the event of force majeure.
Hosted security
The solution provides a high degree of individual component and systemwide security. Customer data is protected through multiple layers of security across the application, transport, network, and physical layers.

Adobe Connect hosted is TRUSTe and SafeHarbor certified. Additionally, Adobe conducts regular security and vulnerability audits, executed by internal security personnel and third-party firms, to validate the security of the hosted infrastructure and software. The audit results are reviewed internally, and any issues identified during this process are addressed in a timely manner to maintain the overall integrity of the service and help ensure the security of customer data.

Hosted architecture
The hosted infrastructure uses a high-availability model. Multiple Adobe Connect servers are clustered behind a hardware load balancer. Connections on this deployment are fast because they are routed to the most available application server in the cluster. In the unlikely event of system failure of any application server, the client connection fails over to a healthy server.

This is true whether the client is working with on-demand content or interacting in real time in an Adobe Connect meeting. Adobe Connect hosted has multiple instances deployed in multiple data centers across the globe to allow great scalability and optimal customer experience.

The Adobe Connect hosted environment also deploys dedicated streaming servers used only for large-scale (600+ connection) seminars.

The following diagram depicts an overview of cluster infrastructure for one of multiple deployments within the Adobe Connect hosted environment. Security, redundancy, failover, and global performance are key considerations in the design, delivery, and regular improvements of the hosted service.

Licensed solution
A licensed solution is available to deploy Adobe Connect Server in your own corporate network. The Adobe Connect Server on-premise model provides the following advantages:

- Long-term cost savings based on software ownership
- Deployment behind a firewall
- Internal hardware and IT personnel for delivery and management
- Integration with existing enterprise infrastructure (LDAP, SSO, and so on)
- Custom configuration settings (such as bandwidth limits)
Licensed architecture
Depending on your organization’s size, projected Adobe Connect Server use, and how crucial Adobe Connect Server is to your business, you can deploy Adobe Connect Server in either single-server or highly redundant clustered configurations. For small- to medium-sized companies with simple network configurations, a dedicated single-server deployment is a viable solution. However, organizations that require high availability can deploy Adobe Connect Server in a cluster. This configuration is ideal for organizations that have many users and are concerned about the load on a single server, or for those that want a redundant system in the event of a single-node failure.

When you deploy Adobe Connect Server in a cluster, clients connect to an Adobe Connect Server farm behind a load balancer. Because Adobe Connect Server separates the network access layer from the application layer, clustering provides the following advantages:

- On-demand stream caching
- Connection aggregation
- Multi-tier architecture

The Adobe Connect Server cluster connects to a database solution: either a single SQL database or a SQL cluster for increased transaction performance and reliability.

To use SSL, implement your preferred solution across a single or clustered Adobe Connect Server deployment. You can also include additional components in the overall deployment—such as integrations with your customer relationship management (CRM) system or Learning Management System (LMS), telephony bridge, or directory service provider to synchronize LDAP user accounts with Adobe Connect Server.

Ports and protocol information

Firewalls, proxies, and ports
The Adobe Connect Server licensed solution works with standard enterprise firewall (proxy) configurations and can also be implemented in the DMZ (perimeter network). Reverse proxies, however, are not yet certified for use with Adobe Connect Server. Adobe Connect Server uses standard communication protocols, so it works like any other application or web server and does not cause problems with network devices. Adobe has been successful in all standard deployments of Adobe Connect Server at customer sites.

The client initiates all communications with Adobe Connect Server. The Adobe Connect Server system uses inbound ports (from the Internet) 80, 443, and 1935 and outbound port (to the mail server) 25.
Managed services deployment
To allow organizations to enjoy the best features from a hosted deployment, without sacrificing the flexibility offered by a licensed deployment, Adobe and key partners offer a managed services deployment. With a managed services, a single tenant server, or cluster of servers, is deployed within a hosted environment. This provides a number of advantages. First, you can integrate the server with services such as LDAP for user management, single sign-on, sharing from videoconferencing equipment, and more. You can also modify the default Adobe Connect configuration files to adjust settings such as bit-rate limits, time-outs, port usage, and other account-specific options. And you get to choose where you would like the server to be located (based on available locations) and exactly when you would like to upgrade to the latest versions and patches offered by Adobe to better align with your own rollout schedules.

Enterprise integration

User administration
Administrators can define managers and team members in Adobe Connect Server, as well as customize the attributes included in user profiles. You can change any attribute of an existing user profile field, set a required field, or add a comment for a field.

A user profile field is an attribute of your organization’s Adobe Connect Server user profile. The customization feature in Adobe Connect Central lets you access user profile fields and attributes in three ways:
- By selecting one or more components from the default list that Adobe Connect Server provides
- By selecting additional components from a list of predefined fields
- By creating your own custom components

The fields for First Name, Last Name, and E-mail are all required for Adobe Connect Server—you cannot select, remove, or modify them. However, you can modify any other existing field to designate it as required and to include a descriptive comment, and do the same for any new fields that you create. You can also move a component up or down in the profile list, depending on its importance.

Adobe Connect Server allows administrators to define policies for password management that are consistent with industry best practices, including administrator password resets and special character requirements. These policies are enforced across the Adobe Connect Server applications and allow administrators to align Adobe Connect Server with their existing security policies. An administrator can govern the details that pertain to the organization’s Adobe Connect Server account through the Administration tab in the web-based Adobe Connect Central.

To learn more about Adobe Connect Server user administration, see the Adobe Connect User Guide available online at www.adobe.com/go/connect_documentation_en.

Adding users and groups
You can use three methods to add users and groups to your Adobe Connect Server implementation. These methods make user management much easier than manual account definition.
- Use LDAP synchronization, which is described in detail in this overview.
- Import users and groups using CSV files. If an organization’s directory has a utility for exporting users and groups to CSV format, an administrator can use the web-based Import feature to import the file into Adobe Connect Server.
- Write custom scripts for user creation or other Adobe Connect Server administration tasks using the Adobe Connect web services API.
LDAP synchronization
For licensed and managed services deployments you can import users and groups into Adobe Connect Server from existing directories with compliant LDAP structures. You can use LDAP or secure LDAPS.

Adobe Connect Server connects as an LDAP client to an LDAP directory, imports users and groups, and synchronizes information about these imported users and groups in the Adobe Connect Server database with the external LDAP directory. Integrating Adobe Connect Server with a directory server allows administrators to avoid manually managing users within Adobe Connect. User and group accounts are created automatically in Adobe Connect Server through manual or scheduled synchronizations with an organization’s directory service.

In addition to synchronizing user profile and group information from an LDAP directory, Adobe Connect supports LDAP-based authentication. This is described in more detail in the "Login administration" section.

HTTP-header is another possible authentication method; it provides users with an automatic, single sign-on (SSO) experience for Adobe Connect Server. Users who are logged in to their desktop using their network username and password can then access Adobe Connect Server services directly, bypassing the Adobe Connect Server login screen.

Login administration
If native authentication (user credentials stored in the Adobe Connect database) is selected, you may also choose to have Adobe Connect Server automatically send new users an email with a link to set a personal password.

If directory service integration has been configured, the recommended method for managing user access is LDAP-based authentication, which leverages the Microsoft® Windows® login credentials to access the Adobe Connect application.

For licensed and managed services deployments, using the Microsoft authentication protocol, NT LAN Manager (NTLM), administrators can configure one directory server for LDAP-based user authentication (advanced configurations are possible to configure more than one directory server). The configuration can point to one or several branches of the directory service if enabled. Adobe Connect users are authenticated directly against the LDAP directory server using their Windows login credentials. After successful login, they are granted access to the Adobe Connect application.

For additional information on Adobe Connect Server directory service integration and LDAP and SSO configuration (HTTP header authentication), see the Migrating, Installing, and Configuring Adobe Connect guide, available at helpx.adobe.com/adobe-connect.html. For a list of the supported LDAP directory servers, see helpx.adobe.com/x-productkb/multi/system-requirements-connect.html.

HTTP header-based authentication uses extra fields in the header of an HTTP request for user authentication. In this configuration, all Adobe Connect Server requests must first be routed to an authentication proxy (reverse proxy) positioned between the client and the Adobe Connect Server. The proxy server authenticates the request and adds an extra HTTP header field. Adobe Connect Server uses the header information to identify the user. If the user passes the authentication test, Adobe Connect Server creates a valid session and allows the user to begin using the system.

Compliance and control
Organizations operating in regulated industries are required to comply with government, and sometimes internal, policies and procedures to ensure compliance. These standards and internal policies dictate how and when employees can communicate and whether the organization must record and archive communication. For example, some organizations are required to log all communications that take place on their networks. Organizations can also choose to retain communications between employees or between employees and external users to meet standards of internal control.

To enable leading organizations to deploy web conferencing in a secure and compliant fashion without spending more on new systems, Adobe Connect offers built-in options that give administrators control over the meeting experience and the options accessible to meeting hosts and meeting participants.

Compliance and control settings are global settings that take effect across an entire system or hosted account (note that some compliance features might not be available to hosted customers).
Three major areas are covered:

- **Disable undesired functionality**—Administrators can turn off certain functional modules, named pods (Pods Management), or sharing features (Share Settings) so that they cannot be used in any meeting.

- **Record and retain communications for auditing purposes**—Administrators can lock down the recording settings for all meetings, log all chat messages in files, and show a custom notice or disclaimer to all participants (Recordings and Notice).

- **Control access to meetings**—This functionality is offered to both administrators and meeting hosts. Hosts can completely disable guest access so that guests can no longer request entry. Hosts can also automatically deny access to specific users and groups. Unlike the two previous categories, meeting access control settings are enforced on a per-meeting basis, not for the entire system or hosted account.

For additional information on Adobe Connect Server compliance and control options, see the *Using Adobe Connect Guide* available online at www.adobe.com/go/connect_documentation_en.

**Learning Management System**

The Adobe Connect Server solution allows you to deploy an enterprise training solution using Adobe Connect Server tools and your existing LMS. You can develop content in tools such as Adobe Presenter, Adobe Captivate, or your existing industry-standard instructional design tool, and host that content either on your LMS or on Adobe Connect Server. Web services APIs allow you to integrate the Adobe Connect Server system with your LMS for coordinated course and training management.

Adobe Presenter is a content authoring tool that allows nontechnical subject matter experts to rapidly create eLearning content from Microsoft PowerPoint. When Adobe Presenter content is deployed in conjunction with an LMS, eLearning can be launched and tracked from the LMS. Adobe Presenter content can be output in either Aviation Industry CBT Committee (AICC) or Sharable Content Object Reference Model (SCORM) formatting standards. An author can select the appropriate LMS standard when publishing content from Adobe Presenter.

In addition, Adobe Presenter offers several advanced settings for how presentations integrate with LMSs. The settings let you specify which data is sent to the LMS and how the data is formatted. Typically, advanced LMS users use these settings or LMS administrators request them. For more details, see the Adobe Presenter User Guide (available online at www.adobe.com/go/connect_documentation_en) or the Adobe Connect Resource Center, which has instructions on how to integrate Adobe Presenter content with commonly used LMSs.

The Flash Media Gateway connects to a telephone conference provider via a SIP proxy.

Enterprises can integrate Adobe Connect Server content in their LMSs. Adobe Connect Server supports AICC with HTTP AICC Communication Protocol (HACP), versions 2.0 through 3.5, a standard LMS communication protocol.
Although Adobe Presenter can generate AICC and SCORM content, the Adobe Connect Server internal LMS only supports and tracks third-party or custom content that conforms to AICC specifications. In addition, Adobe Connect Server can host content created with other tools, such as Adobe Captivate and Adobe Authorware. In Adobe Captivate and Adobe Presenter, selecting the reporting option provides more detailed reporting information. Adobe Connect Server can also accept any content that adheres to the AICC interaction standard. If assessments or surveys are deployed, Adobe Connect Server can track completion and score data. It can track individual question reporting with some additional content development work.

Audio conferencing integration
Adobe Connect has built-in Voice over IP (VoIP), and it also integrates with audio conferencing systems via two key features:

- **Universal Voice**—The ability to merge the VoIP function of the Adobe Connect meeting with a telephone-based audio conference. This enables hosts to broadcast the telephone-based audio conference in the web meeting and to use the Adobe Connect meeting room to pass VoIP audio into the telephone conference, turning the Adobe Connect meeting client into a softphone.

- **Conferencing service provider adaptors**—Vendor-specific telephony adapters that provide the ability to control all aspects of the audio conference such as starting and stopping a conference call, muting selected users, and so on. In addition, the adapter provides real-time indicators for current speaker and dial-in status.

For licensed customers, Universal Voice is enabled by configuring the Flash Media Gateway (FMG) portion of the Adobe Connect Server to connect to a telephone conference provider via a Session Initiation Protocol (SIP) proxy available within your organization. The Flash Media Gateway acts as a SIP User Agent and can initiate multiple calls on behalf of many Adobe Connect meeting rooms. In a cluster environment, the FMG component can be externalized to a dedicated server. FMG servers can also be clustered. One FMG server can handle up to 400 concurrent calls equivalent to 400 simultaneous meetings regardless of how many people are in each meeting.

The in-meeting call control feature is enabled by configuring the various telephony adapters provided with Adobe Connect. Each telephony adapter is a Java component that connects via TCP/IP to the API interface of the audio bridge to synchronize the audio conference and the web conference.

Videoconferencing integration
Adobe Connect integrates with SIP-compliant videoconferencing hardware, allowing you to leverage your existing hardware-based videoconferencing solutions and stream video into Adobe Connect meetings. Now viewers can attend from anywhere on virtually any computer without installing a dedicated viewing application.

Videoconferencing integration is also enabled by configuring the Flash Media Gateway portion of the Adobe Connect Server to connect to a SIP-enabled video device and to receive an H.264 video stream. Adobe Connect then replicates that stream for all users in the meeting.

The Flash Media Gateway allows Adobe Connect to stream content from a SIP-compliant video device.
Additional components
Adobe Connect offers a number of additional components as plug-ins to Microsoft Outlook, Microsoft Lync, and Lotus Notes. These components enable meeting hosts to quickly invite participants to new or existing Adobe Connect meetings directly from within these popular scheduling and messaging applications.

For information on Adobe Connect downloads and updates, visit www.adobe.com/support/connect/downloads-updates.html.

Extensibility and custom integration
Adobe Connect Server is highly customizable and extensible, with support for custom branding, directory services integration, system extensibility, bidirectional data integration, and meeting extensibility. Adobe Connect Server enables system extensibility with application interfaces that integrate web communication capabilities with the application network, including integration with enterprise portals, reporting applications, CRM systems, learning and content management systems, and other corporate systems. Adobe Connect Server also provides support for custom applications and components. Through published APIs, organizations can incorporate external data and functionality directly with Adobe Connect Server. Using the Collaboration Builder SDK, you can also extend the functionality of any meeting room, seminar room, or virtual classroom. The SDK allows you to build multiuser applications such as games, content authoring tools, or media viewers that operate collaboratively from within your meeting.

Web services APIs
The Adobe Connect Server platform provides the infrastructure that training, events, and meeting applications use. With the web services APIs, you can extend and integrate these applications by using a complete web services framework. You can incorporate Adobe Connect Server functionality and reporting information directly into third-party systems such as portals and CRM and enterprise resource planning (ERP) systems. You can use web services to manage the full breadth of the solution, including everything from user management to in-depth reporting on application use.

Consider the following scenario to understand the possibilities of custom integration. You have an existing user management system of record, such as LDAP, Microsoft Active Directory, or another third-party system. This central user management system is deployed in your corporate infrastructure and is an integral part of existing business processes. You want to use your existing investments across all solutions that you deploy, including Adobe Connect Server. The Adobe Connect Server XML web services allow complete user management by an external system, such as a directory service. You can write an application that synchronizes users between these two systems. For example, you could write an application based on J2EE (or another technology of your choice) that pulls a list of users from the directory namespace, compares this list against a list of Adobe Connect Server users, and then performs requested updates in the Adobe Connect Server user repository, such as adding or deleting users and groups in Adobe Connect Server. This is just one example of how you might build integration or extend the Adobe Connect Server feature set. Check the Adobe Connect Developer Center at www.adobe.com/devnet/adobeconnect for more XML web services examples.

To use web services, you must be able to communicate with Adobe Connect Server over HTTP or HTTPS, depending on whether you have enabled SSL. You call Adobe Connect Server web services and pass in one or more parameters—either as name-value pairs or as an XML package—and the web service returns a complete XML document, which can then be parsed and leveraged as necessary in your external applications.

Note: If you use the hosted service, you can also take advantage of Adobe Connect Server extensibility by using XML web services. However, you must abide by the terms of service, which restricts certain activities, such as bulk user imports. Instead, you must add each user into the system individually or by importing a CSV file.
You can use web services for the following features:

**Access control**—In many situations, content requires strict access control to ensure that information is secure and reaches only its intended audience. Adobe Connect Server allows external systems to authenticate, manage users, set permissions, and so on—all through the web services framework.

**User management**—You can take advantage of existing directory services by developing synchronization processes between your directory service and Adobe Connect Server. You can integrate user profiles, Adobe Connect Server content, and reporting data into external systems such as an enterprise portal, CRM, and ERP applications.

**Reporting**—You can use the detailed reporting capabilities of Adobe Connect Server in external systems, such as employee performance management solutions or an LMS, to derive real-time reporting from a single reporting infrastructure. Similarly, you can create custom reports using Adobe Connect Server web services.

**Content, meeting, training, and event management**—You can upload content from a custom application into Adobe Connect Server, and you can also create new meeting or collaboration sessions. You can create and manage Adobe Connect Server assets and meetings from any application that uses web services.

**Database views**

Database views let customers create custom reports through common third-party reporting tools such as Business Objects Crystal Reports. Database-level views are read-only; to alter or manipulate Adobe Connect Server information, use Adobe Connect Server XML web services APIs.

**Collaboration Builder SDK**

Adobe Connect allows you to add functionality to your meeting rooms, seminar rooms, and virtual classrooms in much the same way that you can add functionality to your smartphone with additional apps. These apps could be used for creating or editing content, multiuser games, learning interactions, or streaming media viewers. The apps within Adobe Connect are called custom pods and can be authored by anyone using the Flex development environment. The Adobe Connect Collaboration Builder SDK is a free library of components that you can install within a Flex authoring environment. These components allow software developers to build a collaborative application that can be loaded as a custom pod within an Adobe Connect meeting room. Custom pods can allow different meeting roles to view different levels of user interface and access different abilities to edit and interact with the application. This lets hosts and presenters view the management user interface for a pod, while participants focus on the interaction or media within the pod. Custom pod applications can also communicate with external web services to display and edit data or media stored remotely.

For examples of these applications, visit the Adobe Connect extensions page at www.adobe.com/products/adobeconnect/extend.html#3. For more information on developing custom pods, visit the Adobe Connect Developer Center at www.adobe.com/devnet/adobeconnect.html.
Adobe Connect Edge Server
Adobe Connect Edge Server provides stream consolidation, content caching, network-edge deployments, and more control over the flow of information. These benefits serve two purposes. Edge servers enable enterprises to expose the Adobe Connect service to external clients in a DMZ while the server and data are securely deployed beside IT security. They can also be deployed to provide bandwidth consolidation in certain scenarios.

Architecture
Traditionally, users connect directly to the primary Adobe Connect Server or cluster, which handles authentication, access control, and on-demand and real-time video, audio, and data delivery. The communication, as demonstrated in the following example, results in 1,000 individual connections between clients and the server. If you take this deployment further and consider regional office connections, these additional clients initiate direct connections to Adobe Connect Server as well. This additional traffic results in high-bandwidth requirements between the regional offices and the primary server, and potentially increases latency during the meeting experience.

Demand for connections increases when Acrobat Connect Server serves multiple regional offices and many users.

Edge servers address this deployment concern by consolidating regional office streams before they connect to the primary server. Instead of one stream per user, it is limited to one stream per meeting. Organizations can also cluster edge servers to provide system redundancy and increased capacity at the edge. Requests for HTTP-based content (such as on-demand content or courses) are not combined, but the results are cached so that requests for that content do not result in multiple requests to the server. This caching not only dramatically reduces network traffic, but it also reduces load on the origin Adobe Connect Server or cluster. The following example shows how bandwidth consolidation is achieved for an employee all-hands meeting.

All users at the edge are attending the same employee all-hands meeting. Lowered demand on the origin Adobe Connect Server cluster occurs when edge servers are deployed. Connection aggregation occurs on a per-meeting basis.
Data flow
Adobe Connect Edge Server is designed to allocate and balance access to Adobe Connect Server by using existing bandwidth resources more efficiently. After the edge servers are deployed, users access Adobe Connect Server through their configured edge server. Edge servers forward authentication requests to Adobe Connect Server, but after they are authorized, and if the data requested is found in the edge server’s cache, the edge server returns the cached meeting or training content data to the requesting client (the user’s computer) without calling on Adobe Connect Server. This detour to Adobe Connect Server is transparent to users. In this scenario, aside from authentication, no additional demands are placed on the origin servers.

If the requested data is not found in the edge server’s cache, the edge server forwards the client’s request to the origin servers, where the user is authenticated and the request for services is authorized. The origin servers return the results to the requesting edge server, which in turn delivers the results to the requesting client. The edge server also stores this information in its cache, where other authenticated users can access it. In this scenario, fewer requests for services are forwarded to the origin servers.

An edge server is configured to intercept the requests for Adobe Connect Server services from a particular zone. Adobe Connect Edge Server then collects or aggregates these requests and transmits them to the origin servers (see the following example for data flow with edge servers). The origin server returns the results to the edge server, which forwards the data to the user’s client computer.

Sample scenario
A networked Adobe Connect Server deployment has an edge server installed. One edge server aggregates and forwards requests from San Francisco to an Adobe Connect origin server deployed in Chicago. Each edge server then performs the following steps:

- Gathers the requests from its clients for each meeting and forwards them to the origin servers located in the data center in Chicago
- Receives the responses from the origin
- Transmits and distributes responses to the clients in each zone
Deploying servers in a cluster
Adobe Connect Server offers true enterprise-class scalability with support for single server or clustered environments. Organizations that require high availability can choose to deploy Adobe Connect Server in a cluster. Clusters provide reliable, redundant deployment that can support thousands of concurrent users.

An Adobe Connect Server cluster is made up of identical components for which each server provides identical functionality. If one server fails, the request is transparently routed to the next. This routing is easily accomplished because Adobe Connect Server on demand and real-time data is replicated across multiple servers for redundancy.

Adobe Connect Server is designed so that no single point of control or single point of failure exists. Because of this design, you can add or remove servers from your cluster and scale your Adobe Connect Server deployment to meet your organization’s needs.

In an Adobe Connect Server cluster configuration, typically a load balancer (or SSL hardware accelerator) is placed in front of each server farm, where each HTTP connection request is selected by round-robin. HTTP requests are stateless, ensuring that a server failure does not affect the uptime of the system. RTMP connections, such as Adobe Connect meetings, do not go through the load balancer. Instead, the Adobe Connect Server application server uses a reservation algorithm to select the appropriate servers for the primary meeting instance and the backup instance. A meeting uses health checks to manage the failover process between the servers.

To provide redundancy and instant failover, when each meeting is instantiated, a primary server is chosen to host the meeting and a secondary server is chosen as the backup. If the primary server hosting the meeting fails, all meeting attendees are reconnected to the backup server, and the meeting continues with the same content and environment.

Shared storage
Adobe Connect Server can store content on network-attached storage (NAS) and storage area network (SAN) devices. Content is any file published to Adobe Connect Server, such as courses; SWF, PPT, or PDF files; and archived recordings.

When you use shared storage, you can configure Adobe Connect Server to use the server’s disk as a content cache so that all content is copied to the external storage device and pulled to each server’s content folder as needed. Old content is purged from each server’s content folder to make room for new content as needed (the content is always kept on the NAS or SAN device). This configuration frees resources on the application server, which is especially helpful in a large cluster.

If you don’t configure a content cache, content is mirrored on all servers and the external storage device. When an external storage device fills up, you can add more space to the device or add another device to the front of the chain. Content only writes to the first device in the chain.

Database server clusters
When deploying Adobe Connect Server in a cluster, the database must reside on a different computer than Adobe Connect Server in a separate database layer. The database can be either a single SQL Server instance or a SQL cluster. Furthermore, all Adobe Connect Server servers in the cluster must have access to the database.

A cluster configuration reduces the load on a single computer and enables failover and backups without disrupting service.

Edge server clusters
Adobe Connect Server enables organizations to support edge networks through Adobe Connect Edge Server. Edge routing reduces the bandwidth for large meetings, and edge servers support stateless failover.

Event server clusters
Multiple Adobe CQ publisher instances can link to a single author instance for load balancing and higher availability. Multiple Adobe CQ author instances can be clustered for load balancing and failover capability. See the "Sizing licensed deployments" section for more information.
Sizing licensed deployments

The main factor when sizing a licensed deployment of Adobe Connect is peak concurrent users-the maximum number of users that the system will have to support during the week. This number affects the number of servers required (CPU capacity) and the needed bandwidth.

To get to this number, it is important to understand how Adobe Connect will be used-for general collaboration, live classrooms or seminars, or on-demand training? Each of these use cases is different, and the calculation for the maximum peak user will differ.

Meetings

General collaboration or ad hoc collaboration are sized using a probabilistic model similar to the one used for sizing up telephony systems. Within the population of Adobe Connect users, how many will decide to hold an Adobe Connect meeting at the same time with how many people?

As a rule of thumb, here is the correlation we have observed between user population and peak concurrent users:

<table>
<thead>
<tr>
<th>Adobe Connect User Population</th>
<th>Peak Concurrent User</th>
</tr>
</thead>
<tbody>
<tr>
<td>100–1,000</td>
<td>20%</td>
</tr>
<tr>
<td>1,001–5,000</td>
<td>15%</td>
</tr>
<tr>
<td>5,001–10,000</td>
<td>10%</td>
</tr>
<tr>
<td>10,001–100,000</td>
<td>3%</td>
</tr>
<tr>
<td>100,000 and above</td>
<td>1%</td>
</tr>
</tbody>
</table>

Virtual classrooms and seminars

Training classes and seminars are usually scheduled ahead of time with an identified number of people, so sizing is more deterministic. Organizations can predict attendance based on registration and how many classrooms are running concurrently.

In these cases, obtaining the peak concurrent user number is easy. Just find the maximum live classrooms or seminars that can run at the same time during the week, and add up all the participants. When using a combination of ad hoc collaboration and live classrooms or seminars, the peak concurrency numbers are additive for each use case. It’s recommended to add 30% breathing room to account for spikes or expanded usage.

The peak concurrency number can then be used to derive the number of servers required. An Adobe Connect Server has been tested to support up to 1,500 users in a meeting, but a conservative guideline is one Adobe Connect Server for every 500 concurrent users.

Bandwidth requirements depend on the type of usage, such as screen sharing, uploads, and video. Refer to the tables at the end of this guide for suggested bandwidth requirements. Our experience across use cases shows that 40Kbps of bandwidth per concurrent user is a good rule of thumb. Further bandwidth analysis might be required to size the impact on WAN or LAN based on where people are accessing the meeting from.

Sizing for events and registration

Events are logically divided across two types of servers-authoring and publishing-the first of which is for creation of HTML pages, which are automatically replicated to the publishing server for public access. A single Adobe CQ event authoring server node can support approximately 30-35 concurrent event publishers. A single Adobe CQ event publishing server can support one user per second during registration activities, and up to three users per second for login to an event.

Sizing for on-demand content

On-demand content is sized differently than live meetings. The key is how many people will try to access content within the same 2-second interval. Each Adobe Connect Server can support 125 simultaneous requests. If servers are clustered, the maximum number of simultaneous requests is 500, which allows up to 15,000 requests for on-demand content within 1 minute. Servers required by on-demand content would be in addition to the servers required for the live meeting scenario.
Security
The easiest solution to secure a dedicated, single-server Adobe Connect Server system is to block all ports except 443 (for SSL-enabled traffic) configure Adobe Connect to use software or hardware SSL, and allow only HTTPS and RTMP connections. An external hardware firewall appliance provides an additional layer of protection against gaps in the operating system.

Multiserver (cluster) solutions are inherently more complex. You can configure and extend the Adobe Connect Server service with geographically dispersed edge servers. However, you must understand how to secure the communications between the origin cluster and edge clusters. Following are suggestions for securing multiserver solutions:

- Create an extra subnet for the Adobe Connect Server system. For multiserver solutions in a single location, a private network is simple and offers a high level of security.
- Use a local software firewall. For a clustered Adobe Connect Server system that shares a public network with other customer servers, you might find that a software firewall is appropriate on each individual server.
- Configure SSL. You can use SSL to secure communications between the Adobe Connect Server edge servers and the origin Adobe Connect Server.

Web server security
Adobe Connect Server relies on Apache HTTP Server for its web server functionality. The server is hardened in the Adobe implementation.

Secure Sockets Layer and Transport Layer Security
You can deploy a licensed version of Adobe Connect Server with an SSL layer in one of two ways: a software-based solution that uses the native support for SSL in Adobe Media Server, or a hardware-based solution that routes all communication through an external SSL accelerator, which you must purchase separately through your preferred vendor.

Without SSL, all logins are conducted over HTTP connections, and all subsequent content and meetings are delivered over standard unencrypted HTTP and RTMP connections. You can configure SSL to encrypt the HTTP connection, the RTMP connection, or both the HTTP and RTMP connections.

SSL hardware accelerators intercept traffic on port 443, decrypt the information, and send it back to Adobe Connect Server over a port and IP address that is presumably not exposed outside your corporate security measures. The server has no indication that the original data was encrypted. Adobe has tested and verified Adobe Connect Server with the following SSL hardware accelerator providers:

- F5 Big-IP 1000
- Cisco Catalyst 6590 Switch
- Radware T100

In the hosted solution, SSL is enabled for login and content management. SSL for realtime communications is an available option on a per-account basis.

You can use a software-based SSL, but Adobe recommends hardware accelerators for better performance. For details on setting up a software-based SSL solution with Adobe Connect Server, see the Migrating, Installing, and Configuring Adobe Connect guide at helpx.adobe.com/adobe-connect.html.

Your network configuration and environment has a direct effect on Adobe Connect Server performance, and these variables ultimately determine how Adobe Connect Server should be deployed with your SSL hardware. Adobe Connect Server might support other solutions in the industry, but the providers listed are the only ones that are confirmed at this time.
Public key infrastructure
You can set up a public key infrastructure (PKI) to manage identification credentials as part of your Adobe Connect Server security architecture for clients. In the more familiar SSL protocol, the server must verify its identity to the client. In PKI, the client must verify its identity to the server.

A trusted third party, called a certification authority, verifies the identity of a client and binds a certificate in X.509 format (also called a public key) to that client. When a client connects to Adobe Connect Server, a proxy negotiates the connection for PKI. If the client has a cookie from a previous session or has a valid certificate, the client is connected to Adobe Connect Server. Use HTTP header-based authentication to implement PKI.

Database security
Whether or not you are hosting your database on the same server as Adobe Connect Server, you must be certain that your database is secure. Computers hosting a database must be in a physically secure location. Additional precautions include installing the database in the secure zone of your organization’s intranet, never connecting the database directly to the Internet, backing up all data regularly, and storing copies in a secure off-site location.

To further secure your Microsoft SQL database, see the Microsoft security website (www.microsoft.com/sql/technologies/security).

The Adobe Connect Server application server is designed to prevent unauthorized remote access to the database. Adobe Connect Server uses only prepared statements to communicate with the database, thereby preventing the most common remote SQL exploits. Adobe Connect Server further checks the validity of arguments to the database and finally performs a security check on each access to every key in the database. The Adobe Connect Server security system’s default behavior is to deny access where permission is not explicitly granted to a given row.

Adobe Connect Server also encrypts columns in the database that contain sensitive data. Even someone with full access to the database server is not able to access user passwords or other sensitive information.

Adobe Connect Server supports SQL authentication only. You must select SQL Server with mixed-mode authentication. Adobe Connect Server does not support Windows Authentication mode.

Content access
Adobe Connect Central is a web application that acts as an access and control point for all Adobe Connect Server applications. Adobe Connect Central not only allows you to set up and manage meetings, seminars, and training courses and curriculums, but it also enables you to manage and control content that you can share through meetings, presentations, training courses, and events.

To secure content, you can use the user management component of Adobe Connect Central to set access permissions for the users of the content and the administration of the content itself through a simple, intuitive user interface. All Adobe Connect Server content is contained and organized in a directory of folders called the Content library, which you access through Adobe Connect Central.

Furthermore, not everyone can use all the Adobe Connect Central features. These access controlled features depend on the Adobe Connect Server configuration and each user’s permissions. For example, if a user is not a member of the Administrators group, they cannot access the Administration tab in Adobe Connect Central. For more information on securing content and working with the content library, see the Using Adobe Connect guide, available online at helpx.adobe.com/adobe-connect.html.

Hosting Adobe Connect Add-in
Adobe Connect Add-in is a version of Flash Player that includes enhanced features for Adobe Connect meetings, such as screen-sharing capabilities. When Adobe Connect Add-in is required, it is downloaded from an Adobe server in a seamless process that is hidden to the user. However, if your organization does not allow employees to download software from external servers, you can host Adobe Connect Add-in on your own server.
Adobe Connect bandwidth requirements
Adobe Connect optimizes communications and reduces bandwidth through the following mechanisms:

- **TCP-based streaming**—All rich content, including audio, video, screen sharing, and software simulations, is streamed.

- **Compressed content**—Regardless of the bandwidth available, Flash Player compatible content is highly compressed to reduce the effect on the network.

- **Vector graphics**—Flash Player compatible graphics, text, animations, and images are automatically resized in the viewing window, thereby maintaining image quality.

- **Incremental image differentials**—When screen sharing and running live video, Adobe Connect Server sends only incremental image differentials.

- **Audio control**—Adobe Connect Server offers audio options for controlling your existing infrastructure: high-performance PC-to-PC (VoIP) or integrated conference calling.

- **Edge servers**—Deploying Adobe Connect Edge Server increases the efficiency of global network traffic by consolidating bandwidth from edges to origins.

The table found in Exhibit A represents the bandwidth required during an Adobe Connect Meeting.

The client bandwidth characteristics are detailed by feature in kilobits per second (kbs). To determine bandwidth requirements, use the following guidelines:

- Estimate the required per-client bandwidth by summing the kilobits per second required for each concurrently used feature.

- Estimate total network bandwidth required for an Adobe Connect Meeting by multiplying the per-client bandwidth by the number of meeting participants.

- Bandwidth estimates are based on a single participant using a feature (for example, one person sharing a camera, not three people sharing their cameras). For several participants using a feature together, multiply the listed bandwidth estimate by the number of people using it.

Uploading PowerPoint and PDF files directly into a meeting uses significantly less bandwidth than screen sharing these documents. Adobe Connect Server automatically converts these formats into a lightweight vector format and display the documents, complete with custom animations and clickable hyperlinks, as high-fidelity documents that can be navigated at length with virtually no bandwidth impact. Once converted, these lightweight documents are delivered via HTTP to each client and displayed in the meeting room in a Share pod. Once they are delivered, very little bandwidth is consumed to keep the meeting view synchronized, change slides, or page through an entire PDF document.

Chat, notes, and whiteboard activities require very little bandwidth. The File Share pod also has no impact on bandwidth when displaying a list of content. If the user downloads the file, the transfer is HTTP, and the impact will depend on document size.
Bandwidth and quality settings
Appendix A describes the settings used and observed bandwidth for each element in a typical meeting scenario. This table is strictly a guideline—bandwidth usage is influenced by a number of factors, and therefore, actual bandwidth may vary.

Additional factors that may influence bandwidth include:

- **Resolution**—A monitor set to 1280x1024 contains approximately 67% more pixels than a monitor set to 1024x768. Therefore bandwidth required to share the higher resolution may be up to 67% greater than for the lower resolution.

- **Color bit depth**—A monitor set to 16-bit will use slightly less bandwidth than a monitor set to 24-bit or 32-bit color depth.

- **FLV video encoding**—Bandwidth required for an uploaded video file is dependent on the bit rate of the preencoded FLV file being streamed and is unaffected by room settings.

- **MP3 files encoding**—Bandwidth required for an uploaded MP3 file will be dependent on the MP3 encoding and is unaffected by the room settings.

- **SIP.XML settings**—For licensed servers, a SIP.XML file defines the quality for configured videoconferencing devices. The choice of quality for each of these devices may result in different bandwidth results than listed in this table.
### Appendix A—Adobe Connect bandwidth observations

#### Adobe Connect 8 Bandwidth Observations

<table>
<thead>
<tr>
<th>Quality Level</th>
<th>Bandwidth (kbps)</th>
<th>Frame Rate (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low quality</td>
<td>184</td>
<td>320</td>
</tr>
<tr>
<td>Medium quality</td>
<td>366</td>
<td>320</td>
</tr>
<tr>
<td>Standard quality</td>
<td>408</td>
<td>640</td>
</tr>
<tr>
<td>High quality</td>
<td>501</td>
<td>640</td>
</tr>
</tbody>
</table>

#### WebCam

<table>
<thead>
<tr>
<th>Quality Level</th>
<th>Resolution</th>
<th>Bandwidth (kbps)</th>
<th>Frame Rate (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low quality</td>
<td>320x240</td>
<td>44</td>
<td>4</td>
</tr>
<tr>
<td>Medium quality</td>
<td>640x480</td>
<td>44</td>
<td>4</td>
</tr>
<tr>
<td>Standard quality</td>
<td>1024x768</td>
<td>44</td>
<td>4</td>
</tr>
<tr>
<td>High quality</td>
<td>1344x1024</td>
<td>44</td>
<td>4</td>
</tr>
</tbody>
</table>

#### Video Telephony

<table>
<thead>
<tr>
<th>SIP Quality Level</th>
<th>Bandwidth (kbps)</th>
<th>Frame Rate (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>736</td>
<td>216</td>
</tr>
<tr>
<td>Medium</td>
<td>576</td>
<td>216</td>
</tr>
<tr>
<td>Low</td>
<td>432</td>
<td>216</td>
</tr>
</tbody>
</table>

#### Bandwidth Limiters

<table>
<thead>
<tr>
<th>Meeting Type</th>
<th>LAN Modem</th>
<th>DSL Modem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full meeting</td>
<td>140</td>
<td>100</td>
</tr>
<tr>
<td>Medium</td>
<td>120</td>
<td>90</td>
</tr>
<tr>
<td>Low</td>
<td>100</td>
<td>70</td>
</tr>
</tbody>
</table>

#### Optimized Room Bandwidth

<table>
<thead>
<tr>
<th>Feature</th>
<th>LAN Modem</th>
<th>DSL Modem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video</td>
<td>140</td>
<td>100</td>
</tr>
<tr>
<td>Whiteboard</td>
<td>60</td>
<td>30</td>
</tr>
<tr>
<td>Chat</td>
<td>60</td>
<td>30</td>
</tr>
</tbody>
</table>

#### Compression

<table>
<thead>
<tr>
<th>Quality</th>
<th>Resolution</th>
<th>Frame Rate (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>320x240</td>
<td>8</td>
</tr>
<tr>
<td>Medium</td>
<td>640x480</td>
<td>8</td>
</tr>
<tr>
<td>High</td>
<td>1024x768</td>
<td>8</td>
</tr>
</tbody>
</table>

#### Frame Sharing

<table>
<thead>
<tr>
<th>File Share</th>
<th>Compression</th>
<th>Quality</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whiteboard</td>
<td>Negligible</td>
<td>Low</td>
<td>320x240</td>
</tr>
<tr>
<td>Chat</td>
<td>Negligible</td>
<td>Medium</td>
<td>640x480</td>
</tr>
<tr>
<td>Whiteboard</td>
<td>Negligible</td>
<td>High</td>
<td>1024x768</td>
</tr>
<tr>
<td>Chat</td>
<td>Negligible</td>
<td>High</td>
<td>1024x768</td>
</tr>
</tbody>
</table>
## Appendix B—SiteCatalyst variable mapping

| eVar# -> | Campaign | Response |晓程网 | Online | Offline | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | Event Registration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventRegistration | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing | EventListing |Event